Mitigating Control Lifecycle

A high amount of time during a SAP GRC project will be spent on defining processes and responsibilities. My suggestion is to think in lifecycles for getting a better understanding of the processes and who is taking over the responsibilty.

In this post I would like to clarify the lifecycle of Mitigating Controls. I have grouped them into four steps Create, Change, Delete and Review. Please see for each step expected Tasks and who is involved.

On request from Colleen I have additionally added the RACI matrix to see who is **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed for each step. Please be aware that this is very much depending on the point of view and can be different in your organization. My considerations are commonsense and pretty much of thinking in smooth processes throughout a global enterprise.

Creation of Mitigating Controls

Tasks

Define the control including:

- Control description
- Control execution
- Control approver and control monitor
- Documentation of control execution
- Reports used to monitor the risk

Involved functions

- Control Owner
- Internal Control responsible
- SAP GRC responsible

Creation of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Control description	I	A	R
Control execution	I	A	R
Control approver and control monitor	I	A	R
Documentation of control execution	R	A	
Reports used to monitor the risk	R	A	

Changing of Mitigating Controls

Tasks

Change the control for example:

- Control description
- Control execution
- Control approver and control monitor
- Documentation of control execution
- Reports used to monitor the risk

Involved functions

- Control owner
- Internal Control responsible
- SAP GRC responsible

Deletion of Mitigation Controls

Tasks

- Delete the mitigating control within SAP GRC AC
- Document the decision of deletion of the mitigating control

Involved functions

- Control Owner
- Internal Control responsible
- SAP GRC responsible

Changing of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Control description	I	A	R
Control execution	I	A	R
Control approver and control monitor	I	A	R
Documentation of control execution	R	A	
Reports used to monitor the risk	R	A	

Reviewing of Mitigating Controls

Tasks

- Analyse if maintained controls within SAP GRC are still valid
- Analyse if the mitigating controls are covering the risk fully

Deletion of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Delete the mitigating control within SAP GRC AC	I	A	R
Document the decision of deletion of the mitigating control	C	R	

Involved functions

- Control owner
- Internal Control responsible
- SAP GRC responsible

Reviewing of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Analyse if maintained controls within SAP GRC are still valid	R	A	C
Analyse if the mitigating controls are covering the risk fully	R	A	
Test the effectiveness of the mitigating controls	R	A	

If you want to have further information or contribute in this blog post do not hesitate to contact me or reply to this post directly.